Центр «Россия-ОЭСР»

Руководство по цифровому комплаенсу для компаний

Американская готика, Грант Вуд, 1930 г.

Июль 2019

РОССИЙСКИЙ ЦЕНТР КОМПЕТЕНЦИЙ И АНАЛИЗА СТАНДАРТОВ ОЭСР

Проект Руководства по цифровому комплаенсу был разработан Центром Россия-ОЭСР, чтобы показать компаниям, работающим в условиях цифровой экономики, те направления работы, которые помогут снизить нефинансовые риски. Документ основывается на международных стандартах, в т.ч. ОЭСР.

Документ подготовлен под руководством Коваль Александры при поддержке экспертов:

Левашенко Антонины

Гирич Марии

Ермохина Ивана

Валамат-Заде Алины

Руководство по цифровому комплаенсу для компаний

Проект Центра Россия-ОЭСР РАНХиГС

Ответственное ведение бизнеса сегодня (ОВБ) – это не просто международный тренд, это требования к поведению компаний, которые часто приобретают законодательный характер на национальном уровне. Несоблюдение этих требований может привести не только к репутационным издержкам, но и к судебным разбирательствам. Требования ответственного поведения предъявляются не только к транснациональным компаниям, но и МСП. И все больше вопросов «Как быть ответственным?» возникает в условиях цифровизации и стремительного развития прорывных цифровых технологий, которые порождают новые вызовы для цифровой безопасности и прав человека. Предотвратить эти и другие нефинансовые риски призван цифровой комплаенс.

Данное Руководство по цифровому комплаенсу было разработано Центром Россия-ОЭСР для того, чтобы показать компаниям, работающим в условиях цифровой экономики, те направления работы, уделяя внимание которым, они смогут снизить нефинансовые риски. Данное руководство основывается на международных стандартах, в том числе ОЭСР.

1. Что такое комплаенс?

Комплаенс означает создание внутренних политик компании, направленных на соответствие нормам закона и стандартам, на снижение внешних рисков. В условиях цифровой экономики, когда ключевым активом становятся данные и основанные на них инновации, особое значение приобретает соблюдение стандартов в области цифровой безопасности и неприкосновенности частной жизни, как это предусмотрено в Рекомендации ОЭСР по управлению рисками в области цифровой безопасности для экономического и социального процветания (2015). Возможность противостоять рискам обеспечивает конкурентоспособность компании и позволяет ей быть устойчивой. Таким образом, решающее значение для компаний приобретает цифровой комплаенс - правила внутренней политики, в первую очередь, IT-компаний, которые направлены на минимизацию рисков цифровой безопасности, неприкосновенности частной жизни и других нефинансовых рисков.

2. Для каких компаний важен цифровой комплаенс?

Цифровой комплаенс важен для всех компаний, не только для IT-бизнеса. Риск, связанный с инцидентами в области цифровой безопасности, вошел в пятерку крупнейших бизнес-рисков в 2015 году (в 2014 кибер-риски занимали 8 место, а в 2013 - лишь 15). В 2019 году – они занимают уже второе место. В условиях цифровой экономики киберпреступность, сбои в работе IT-инфраструктуры, утечки данных могут парализовать работу любой компании. Расширение возможности подключения устройств к Интернету и общей IT-инфраструктуре делает все звенья в цепочке поставок уязвимыми для кибер-инцидентов.

3. Во сколько может обойтись инцидент в сфере цифровой безопасности?

Стоимость типичного инцидента цифровой безопасности составляет около 200 000 дол. США (примерно столько же, сколько годовой бюджет фирмы на IT-безопасность), и это около 0,4% от предполагаемого годового дохода компании. По оценкам McAfee, киберпреступность в 2018 г. обходится в

600 млрд дол. США в год по сравнению с 445 млрд дол. США в год в 2014 г.

4. Цифровой комплаенс важен только для крупной компании?

Исследование Ponemon State of Cybersecurity в США в отношении МСП показало, что наибольшая доля респондентов, которые вообще не соблюдали никаких стандартов или руководств по информационной безопасности, составляет 41%. Очень небольшая часть компаний, участвовавших в опросе (3%), соблюдает ISO 27001/2. 16% респондентов внедрили стандарт NIST Framework, который был разработан для операторов критически важной инфраструктуры, но все чаще используется другими компаниями частного сектора. В 2015 г. в Великобритании опрос PWC по нарушениям информационной безопасности показал, какие стандарты и руководства применяются на практике. Наибольшая доля (51%) ответила, что используют признанные стандарты, такие как ISO 27001. Страны стремятся развивать сотрудничество с IT-отраслью и помогать компаниям в оценке возможных рисков. Например, отраслевая ассоциация IT-компаний TechUK в партнерстве с правительством Великобритании подготовила руководство по оценке экспортных рисков кибербезопасности. Руководство содержит детальную информацию о том, как разрабатывать и внедрять соответствующие программы должной осмотрительности.

5. На минимизацию каких рисков должен работать цифровой комплаенс?

Цифровой комплаенс должен помогать компаниям избегать ключевые риски:

- цифровой безопасности
- нарушения неприкосновенности частной жизни
- другие нефинансовые риски.

6. Какое место в цифровом комплаенсе занимает вопрос охраны персональных данных?

Для работы любой компании в условиях цифровой экономики центральным вопросом становится соблюдение требований законодательства в отношении персональных данных. Европейское законодательство предусматривает широкий набор гарантий для субъектов персональных данных, включая право на забвение, на переносимость данных, соблюдение

которых (с учетом экстерриториального характера Регламента GDPR) становится существенным вызовом для цифровых компаний во всем мире. Обрабатывая данные резидентов ЕС важно помнить о четко прописанных требованиях к реализации этих прав, уведомления (нотификации) о нарушениях. Но не только в ЕС действует экстерриториальное законодательство по персональным данным. США, Китай, Индия и другие страны принимают аналогичные нормы.

7. Нужно ли использовать современные IT-решения для повышения качества комплаенса?

Развитие цифрового комплаенса в компании возможно за счет использования современных IT-решений. Так, например, перевод контрактных отношений в онлайн, а также регистрация контрактов на основе технологии блокчейн позволяет повысить транспарентность деятельности компании и цепочек поставок. Кроме того, проведение анализа контрактных отношений с применением технологии искусственного интеллекта позволяет выявлять финансовые и нефинансовые риски компаний.

8. Для IT-компаний комплаенс ограничивается оценкой цифровых рисков?

Компаниям, работящим в цифровом мире, нельзя думать, что комплаенс ограничивается вопросами цифровых рисков. Сегодня ключевое значение приобретают вопросы соблюдения стандартов ответственного ведения бизнеса, которые затрагивают 9 ключевых сфер: права человека, трудовые права, коррупция, охрана окружающей среды, налоги, конкуренция, наука и технологии, правила раскрытия информации и защита прав потребителей. Эти стандарты закреплены в Руководстве для многонациональных предприятий.

Особенно остро стоит вопрос о соблюдении прав человека IT-бизнесом. Интерес представляет дело в отношении британской компании Gamma International, которая разработала программный продукт Finfisher, позволяющий осуществлять шпионаж. Этот продукт был продан агентствам Правительства Бахрейна, которые использовали его для преследования активистов движения за демократию. Национальный контактный центр (НКЦ) Великобритании пришел к выводу, что компания при

осуществлении деятельности нарушила Руководство ОЭСР, в частности, в отношении прав человека в Бахрейне.

Российские компании, которые экспортируют IT-продукты за рубеж и заключают договоры с зарубежными компаниями, зачастую не знают о требованиях ответственного ведения бизнеса, которые предъявляют страны ОЭСР. Разрешить эту проблему может помочь внедрение цифрового комплаенса.

9. Необходим ли цифровой комплаенс для защиты интеллектуальной собственности?

Выгода, получаемая компанией, может в значительной степени зависеть от защиты ее интеллектуальной собственности. В опросе, проведенном Economist Intelligence Unit, 53% опрашиваемых риск-менеджеров заявили, что нарушение прав интеллектуальной собственности наносит ущерб их компании, а 14% оценили подобный ущерб как серьёзный. Какие факторы риска поможет избежать грамотный цифровой комплаенс? Компания может столкнуться с таким риском, как ненамеренное нелегальное использование чужой интеллектуальной собственности. Например, в результате использования чужих объектов авторского права в своей рекламе; использования дизайна, схожего с дизайном другой компании; установки пиратского программного обеспечения. Кроме того, возможны нарушения прав на интеллектуальную собственность в результате неправомерных действий со стороны партнеров - членов цепочки поставок.

Компания может столкнуться с утечкой конфиденциальной информации и кражей её интеллектуальной собственности в результате доступа к IT-системам или кибератак.

Потенциальными негативными последствиями могут быть срывы в цепочке поставок, возвраты товара и гарантийные претензии, ущерб репутации бренда, судебные процессы, а как результат - судебные издержки и выплаты денежного ущерба. Идентификация и мониторинг подобных рисков может помочь избежать многих негативных последствий вплоть до предотвращения потенциального закрытия компании.

10. Важен ли цифровой комплаенс для электронной коммерции?

Цифровой комплаенс важен для развития электронной коммерции,

которая обеспечивает возможность онлайн-покупки товаров и услуг. Например, внедрение цифрового комплаенса позволяет обеспечивать прослеживаемость в сфере электронной коммерции. Так, компания IBM в сотрудничестве с рядом ритейлеров, включая Walmart и Costco разработала продукт, основанный на технологии блокчейн, который позволяет обеспечивать прослеживаемость пути продукции от поставщика до ритейлера, включая детали производства, проведения инспекций, данных об истечении срока годности, температуре хранения, подробностей доставки и др.

Внедрение цифрового комплаенса позволит повысить эффективность инструментов защиты прав потребителей, борьбы со спамом и недобросовестными практиками в интернете.

11. Как внедрить цифровой компаленс в компании?

ОЭСР в 2018 г. приняла Руководство должной осмотрительности о том, какие практические шаги компания должна сделать для внедрения стандартов ответственного ведения бизнеса. Руководство говорит о следующих шагах:

1) Принять специальный документ – Политику ответственного поведения, направленный на определение и устранение рисков. Стратегия устойчивости SAP, например, определяет шаги, предпринимаемые компанией по обеспечению конфиденциальности и безопасности данных.

2) Сформировать систему оценки потенциальных и фактических рисков проекта. Компания IBM проводит комплексную оценку рисков компании за счет использования современных технологий и проведения опроса около 150 ТОП-менеджеров компании.

3) После определения рисков разработать меры по предотвращению и смягчению последствий. Так, компания Apple приняла программу в области прав человека и ответственного выбора поставщиков, которая включает меры по процедурам должной осмотрительности в отношении поставки конфликтных минералов.

4) Периодически оценивать, какие предпринимаются меры по снижению рисков и какие риски были предотвращены. Компания HP применяет комплексный подход к управлению бизнесом (включая вопросы минимизации рисков

нарушения неприкосновенности частной жизни и цифровой безопасности, обеспечения прозрачности) и использует механизм обратной связи для повышения качества работы.

5) Взаимодействовать с общественностью. Ключевые инструменты: ежегодные доклады предприятия об устойчивости или корпоративной ответственности или другие формы раскрытия информации. Oracle готовит отчет о корпоративной ответственности, в котором раскрывает результаты политики в области ОВБ.

6) Принимать меры по восстановлению в случае наступления негативного воздействия (в случае необходимости). Для того чтобы минимизировать возможные риски, ОЭСР рекомендует использовать механизм страхования кибер-рисков.

Для того чтобы оценить внедрение компанией цифрового комплаенса, мы предлагаем Вам ответить на вопросы, перечисленные в Приложении.

ПРИЛОЖЕНИЕ

Вопросы, на которые должна ответить компания, чтобы оценить эффективность внутреннего цифрового комплаенса:

1. Есть ли в Вашей компании внутренние политики, направленные на предупреждение рисков цифровой безопасности (предусмотрен ли, например, план действий на случай чрезвычайных ситуаций (кибератак))? Руководствуется ли Ваша компания для оценки рисков цифровой безопасности своей деятельности положениями Рекомендации ОЭСР по управлению рисками в области цифровой безопасности для экономического и социального процветания?

2. На какие стандарты, в т.ч. международные (например, как ISO 27001), опирается Ваша компания в ходе реализации мер по обеспечению цифровой безопасности? Проходит ли Ваша компания сертификацию или осуществляет ли Ваша компания аудит внутренних систем безопасности и публикует ли эти данные публично?

3. Есть ли в Вашей компании внутренние политики, направленные на соблюдение законодательства о защите персональных данных? Учитывают ли внутренние политики Вашей компании экстерриториальные требования законодательства о защите персональных данных стран, которые предусматривают необходимость реализации права на забвение, переносимость данных (ЕС), локализации данных (Китай) и т.д.?

4. Приняла ли Ваша компания решение включить стандарты ответственного поведения в политику компании? Если да, то в каком документе сделано соответствующее заявление, и находится ли он в публичном доступе?

5. Есть ли в Вашей компании внутренние политики, направленные на предотвращение рисков в сфере прав человека, основанные на соблюдении Руководящих принципов ООН по вопросам бизнеса и прав человека? Принята ли внутренняя программа по предотвращению нарушений прав человека (осуществляется ли публикация предупреждений о любых потенциальных опасностях для здоровья и безопасности на рабочем месте, осуществляется ли

строгий контроль качества продукции, чтобы предотвратить вероятность того, что она может привести к травме и др.)?

6. Есть ли в Вашей компании внутренние политики, направленные на предотвращение рисков в сфере трудовых прав? Включены ли обязательства по соблюдению прав человека во все стратегии компании, созданы ли механизмы возмещения вреда? Обеспечивает ли Ваша компания соблюдение конвенций МОТ, в т.ч. Конвенции МОТ о минимальном возрасте № 138 и Конвенции о наихудших формах детского труда № 182?

7. Есть ли в Вашей компании внутренние политики, направленные на предотвращение рисков в сфере коррупции? Предусмотрены ли специальные механизмы по противодействию подкупу иностранных должностных лиц в соответствии с Конвенцией ОЭСР по борьбе с подкупом иностранных должностных лиц при осуществлении международных коммерческих сделок и принятыми в ее развитие рекомендациями?

8. Созданы ли в Вашей компании механизмы защиты осведомителей (созданы ли механизмы предоставления информации о фактах правонарушений, определены ли меры защиты осведомителей, включая вопросы компенсации, перевод на другую должность и т.д.)? Является ли Ваша компания участником национальных или международных инициатив по борьбе с коррупцией?

9. Есть ли в Вашей компании внутренние политики, направленные на предотвращение рисков в сфере охраны окружающей среды? Внедрен ли Вашей компанией стандарт ИСО по экологическому менеджменту? Стремится ли Ваша компания к использованию ресурсосберегающих технологий в ходе своей деятельности и в отношении продукции? Стремится ли Ваша компания снизить количество отходов, осуществлять переработку отходов или повторное использование продуктов? Информирует ли Ваша компания общественность о влиянии ее деятельности на экологию, вступает ли она во взаимодействие с общественными организациями в отношении экологических вопросов?

10. Есть ли в Вашей компании внутренние политики, направленные на предотвращение рисков в налоговой сфере, включая возможные злоупотребления положениями налоговых соглашений, нарушения правил трансфертного

ценообразования и др.? Осуществляет ли совет директоров функции надзора за финансовым управлением и стратегиями налогового планирования в целях препятствования вредоносным налоговым практикам (например, стремлению к агрессивному уклонению от уплаты налогов)? Определена ли в Вашей компании политика в отношении выстраивания взаимодействия с налоговыми органами?

11. Есть ли в Вашей компании внутренние политики, направленные на предотвращение рисков в сфере конкуренции, т.е. набор мер, направленных на самоанализ деятельности компании с целью выявления антиконкурентных практик? Оцениваете ли Вы риски нарушения законодательства в сфере конкуренции с учетом использования новых цифровых технологий (анализ больших данных, искусственный интеллект и т.д.)?

12. Есть ли в Вашей компании внутренние политики, направленные на предотвращение рисков в сфере науки и технологий? Осуществляете ли Вы коммерциализацию продуктов, которые заключают в себе новые технологии, в принимающих странах?

13. Реализует ли Ваша компания меры по защите своей интеллектуальной собственности и по предупреждению возможных случаев нарушения прав интеллектуальной собственности третьих лиц? Обеспечивают ли соглашения Вашей компании с контрагентами надлежащую защиту интеллектуальной собственности? Осуществляет ли Ваша компания надлежащую проверку добросовестности контрагента по соблюдению прав интеллектуальной собственности?

14. Есть ли в Вашей компании внутренние политики, направленные на обеспечение раскрытия информации и вовлечения заинтересованных сторон? Созданы ли основы для регулярного взаимодействия с заинтересованными сторонами (работниками, клиентами, НКО и др.) и учета их мнения в процессе управления?

15. Использует ли Ваша компания IT-инструменты и сервисы (базы данных) для оценки благонадежности контрагента, проверки его репутации и нефинансовых рисков? Принят ли в Вашей компании кодекс поведения поставщика, который определяет требования ответственного поведения в отношении потенциальных контрагентов Вашей компании?

16. Работает ли Ваша компания в сфере электронной коммерции (онлайн покупка товаров и услуг)? Если да, то какие инструменты использует Ваша компания для обеспечения прослеживаемости товаров и услуг (например, осуществляет сотрудничество с государственными органами, работает через специальную онлайн систему прослеживаемости, напрямую запрашивает у продавцов сертификаты на товары и проверяет такие сертификаты)? Осуществляет ли Ваша компания борьбу с недобросовестными практиками в интернете, например, борьбу со спамом, борьбу со сфальсифицированными отзывами и потребительскими рейтингами, борьбу с недобросовестной рекламой?

17. Есть ли в Вашей компании внутренние политики, направленные на предотвращение рисков в сфере нарушения прав потребителей? Есть ли в Вашей компании внутренняя система рассмотрения жалоб потребителей онлайн, а также система рассмотрения споров с участием потребителей онлайн?

18. Если Ваша компания ведет деятельность, связанную с развитием технологии искусственного интеллекта (ИИ), учитывает ли она стандарты ответственного развития и использования ИИ, которые определены в Рекомендации по искусственному интеллекту ОЭСР, международных стандартах в отношении ответственного использования данных в рамках создания и развития систем ИИ?

1) Учитывает ли Ваша компания риски нарушения прав человека компаниями, которые работают в области ИИ, поскольку могут возникать ситуации непреднамеренной дискриминации социальных групп (например, женщин, детей, лиц с ограниченными возможностями и др.)?

2) Учитывает ли Ваша компания риски нарушения прав потребителей компаниями, которые работают в области ИИ, поскольку использование ИИ может приводить к злоупотреблениям в отношении уязвимых потребителей (например, азартные игры, предлагаемые азартным людям; психоактивные вещества, продаваемые людям, страдающим от депрессии и т.д.)?

3) Учитывает ли Ваша компания риски нарушения прав потребителей компаниями, которые работают в области ИИ, поскольку системы ИИ могут предоставлять каждому потребителю рекламу, которая с наибольшей вероятностью приведет к желаемому покупательскому поведению с учетом имеющихся данных?

4) Учитывает ли Ваша компания риски того, что алгоритмы ценообразования, заложенные в ИИ, могут приводить к ценовым войнам и сговору с целью получения большей прибыли, даже если изначально это не было заложено?

19. Если Ваша компания ведет деятельность, связанную с развитием технологии блокчейн, учитывает ли она стандарты ответственного развития и использования технологии блокчейн, в особенности, в финансовой сфере?

1) Предусматривает ли внутренняя политика Вашей компании задачу реализации мер по противодействию отмыванию доходов, полученных преступным путем, и финансированию терроризма в соответствии со стандартами ФАТФ?

2) Предусматривает ли внутренняя политика Вашей компании задачу соблюдения экстерриториальных требований законодательства в части оборота и использования цифровых финансовых активов (например, соблюдение требования регистрации и получения лицензии для ведения деятельности криптобиржи)?

3) Предусматривает ли внутренняя политика Вашей компании задачу соблюдения национальных (если применимо) и экстерриториальных требований законодательства в части проведения ICO (например, соблюдение правового режима в отношении регулирования ценных бумаг в случае, если токен имеет признаки финансового актива)?